02890028AA

METHOD AND APPARATUS FOR SELECTIVELY DENYING ACCESS TO ENCODED DATA

ABSTRACT OF THE DISCLOSURE

A method and system is provided for selectively denying access to encoded data. Encryption is used to protect secured data on any of a number of media devices in a system and in which unsecured data is not encrypted. Encrypted and unencrypted data may reside on the same device. Encryption is done by adding an encryption extension to a bus driver, preferably for a SCSI bus. Classified data is determined to be in need of encryption before being stored in a medium. The classified data is encrypted and then transmitted for storage on the medium. Unclassified data is treated as not needing encryption and bypasses the encryption means before being transmitted for storage on the medium. On read operations, non-encrypted data goes directly to the application calling for it. The encryption key is stored only in volatile memory on the target device connected to the medium during a mission. The encryption key is known only in a location physically distance from the target device during a mission. A means is provided for mission personnel to immediately delete the encryption key from volatile memory upon perceiving a threat, as well as a means to automatically delete the encryption key upon a power loss to the target device. When the encryption key is deleted from the target device, the encrypted data is unavailable to any personnel (whether authorized or not) at the location of the target device. Sufficient unencrypted data resides on the target device to enable the target device and mission vehicle to travel to a desired end mission location, thereby enabling mission personnel to get out of "harm's way".

00720T"40E7S960